CLAIMS

1. A system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems, the communication means including a transport entity for providing transport services, and a transport-independent, session-level security entity logically positioned above the transport entity and visible to the local application entity, the security entity being operative to set up secure communication sessions with peer security entities in other systems and comprising:

- key-exchange handshake means for conducting a handshake with a said peer security entity associated with a particular remote application entity with which said local application entity wishes to communicate, this handshake involving the exchange of key-related data for use in generating session keys; and
- secure channel means for enabling messages to be passed between the local application entity and said particular remote application entity with authentication and/or encryption of these messages being effected using the session keys generated from said key-related data whereby to secure these messages in passage between the cooperating security entities;

the handshake means including:

- first means, operative in the course of said handshake, to pass to said peer security entity a first indication indicating the services required by the local application entity, to receive back from said peer security entity a second indication indicating the attributes required of the local application entity by the remote application entity for carrying out said services, and to pass first attribute justifications in the form of one or more certificates, to said peer security entity; and
- second means, operative in the course of said handshake, to pass to said peer security entity a third indication indicating the attributes required of the remote application entity by the local application entity, and to receive second attribute justifications, in the form of one or more certificates, from said peer security entity.

2. A system according to claim 1, wherein the security entity is capable of establishing multiple concurrent security sessions with another system over a common transport connection set up by the transport entity.

3. Please delete claim 3, without prejudice.

4. A system according to claim 1, further comprising attribute justification means for proving from certificates received from the remote system during said handshake that the remote application has the required attributes.

5. A system according to claim 1, wherein said local application entity is a mediation entity acting on behalf of one or more other application entities.

6. Please delete claim 6, without prejudice.

7. A system according to claim 1, wherein the security entity formats its communications intended for the remote peer security entity in protocol data units (PDUs) that each include:

- a session indicator enabling the peer security entity to determine to which security session the PDU relates; and
- a message-type field by which the peer security entity can determine whether the PDU carries handshake-related data or a message being passed over the secure channel of the security session indicated by said session indicator.

---

a'

8. A system according to claim 1, wherein said handshake is a three message handshake, the first message passing from the local security entity to said peer security entity and including said first and third indications, the second message passing from the peer security entity to the local security entity and including said second indication and said second attribute justifications, and the third message passing from the local security entity to said peer security entity and including said first attribute justifications.

9. A system according to claim 2, wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption algorithms that will be subsequently used by the secure channel means for the security session concerned.

10. A system according to claim 9, wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange.

a' cont

11. A system according to claim 8, wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption algorithms that will be subsequently used by the secure channel means for the security session concerned.

12. A system according to claim 11, wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange.

13. A method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport-independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys, the handshake further involving:

- passing from the local security entity to the remote security entity a first indication indicating the services required by the local system, passing from the remote security entity to the local security entity a second indication indicating the attributes required of the local system by the remote system for carrying out said services, and passing from the local security entity to the remote security entity, first attribute justifications in the form of one or more certificates; and
- passing from the local security entity to the remote security entity a third indication indicating the attributes required of the remote system by the local system, and passing from the remote security entity to the local security entity second attribute justifications, in the form of one or more certificates.

14. A method according to claim 13, wherein said handshake is a three message handshake, the first message passing from the local security entity to said remote security entity and including said first and third indications, the second message passing from the remote security entity to the local security entity and including said second indication and said second attribute justifications, and the third message passing from the local security entity to said third security entity and including said first attribute justifications.

15. A method according to claim 13, wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption algorithms to be subsequently used for secure communication between the local and remote systems.

16. A method according to claim 15, wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange.

17. A method according to claim 14, wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption algorithms to be subsequently used for secure communication between the local and remote systems.

18. A method according to claim 17, wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange.

19. A method according to claim 13, wherein each security entity formats its communications intended for the remote peer security entity in protocol data units (PDUs) that each include:

- a session indicator enabling the peer security entity to determine to which security session the PDU relates; and
  a message-type field by which the peer security entity can determine whether the PDU carries handshake-related data or a message being passed over the secure channel of the security session indicated by said session indicator.

20. A method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport-independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys, the handshake further involving:

- the local security entity indicating to the remote security entity the services and attributes required of said remote system by the local system;
- the remote security entity indicating to the local security entity the attributes that the remote system requires of the local system in respect of said services; and
- the exchange of attribute justifications, in the form of certificates, between the security entities.

a' cont

21. A method according to claim 20, wherein said handshake is a three message handshake, comprising:

- a first message passing from the local security entity to said remote security entity and indicating the services and attributes required of said remote system by the local system;
- a second message passing from the remote security entity to the local security entity and indicating the attributes that the remote system requires of the local system in respect of said services, the second message also including attribute justifications provided by the remote system; and
- a third message passing from the local security entity to said third security entity and including attribute justifications provided by the local system.